REMARKS

Claims 1-51 are pending in the present application. In the above amendments, claims 1, 2, 7, 9-11, 14-19, 22, 26-30, 33, 36-40, 43-44, 47, 50, and 51 have been amended to clarify the claimed subject matter. No new claims have been added.

Applicant respectfully responds to this Office Action.

Claim Rejections – 35 USC § 102

Claims 1, 14, 22, 26, and 50

The Office Action rejected independent claims 1, 14, 22, 26, and 50 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,959,393 to Robert L. Hollis et al. (hereinafter "Hollis").

The rejection is respectfully traversed in its entirety.

The Hollis patent discloses a method for securely and dynamically transporting private or sensitive data over existing non-secure networks without overhead and limited security associated with traditional virtual private network (VPN) solutions. In particular, the system disclosed by Hollis describes how non-secured servers are secured by using public-private key cryptography to protect private data transmissions through the servers (nodes).

To clarify the focus of the present claims 1, 14, 22, 26, and 50 have been amended to more clearly recite various features.

To anticipate a claim under 35 U.S.C. § 102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

Applicant submits that Hollis fails to teach a method "wirelessly transmitting the second private key once such that it can be re-created", "wirelessly transmitting the second public key to a verifier device concurrent with transmitting the first public key" and "using the first private key for authentication of the mobile user device."

First, the Final Office Action appears to rely on Hollis, col. 24, lines 39-41, as teaching *wireless transmission of the keys*. However, as illustrated in Fig. 2 of Hollis, the network therein is a wired network and Hollis fails to explicitly state or disclose wireless transmission of keys. By contrast, the present invention operates on a wired network where wireless transmissions of the keys occur as recited in the claims. Because Hollis fails to explicitly teach any kind of wireless transmission as required under 102(e), it fails to teach this recited limitation.

Second, the Final Office Action also appears to rely on Hollis, col. 24, lines 39-41, as teaching wireless transmission of the second public key. However, Hollis makes it clear that the second key pair is an *offline back up* (Col. 24, line 41). Hollis fails to disclose how or if this second key pair is ever transmitted by a mobile user device. In fact, the use of the words "offline back up" appears to indicate that the second key pair in Hollis is not transmitted over the network at all but may be, perhaps, manually accessed or conveyed. Also, Hollis fails to explicitly recite whether the second private key is ever transmitted, since such *off line backup* may simply store the keys. By contrast, the claims explicitly recite that the second public key and second private key are wirelessly transmitted. Because Hollis fails to explicitly teach any

kind of wireless transmission of the second key pair as required under 102(e), it fails to teach this recited limitation.

Third, the Final Office Action also appears to rely on Hollis, col. 24, lines 39-41, as teaching *concurrent transmission of the first and second public keys* as claimed. However, Hollis fails to disclose *concurrent* transmission of the first and second public keys. In fact, Hollis discloses that the second public key backed up offline, which indicates that it is not transmitted at all. Because Hollis fails to explicitly teach concurrent transmission of the first and second public keys as required under 102(e), it fails to teach this recited limitation.

Fourth, the claims as amended now require creating and wirelessly transmitting/outputting the keys from a mobile user device to a verifier device. The Final Office Action relies on the server 246 (Fig. 2) of Hollis as teaching this limitation. However, such server 246 is not a mobile user device and operates on a wired network. This is a clear structural difference between the recited claims and the teachings of Hollis. Consequently, Hollis also fails to teach this limitation.

Claims 29, 30, 43, and 44

The Office Action rejected independent claims 29, 30, 43, and 44 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 7,162,037 to Joerg Schwenk (hereinafter "Schwenk").

The rejection is respectfully traversed in its entirety.

Schwenk describes a method for generating and regenerating an encryption key. In particular, Schwenk discloses an algorithm for allowing a user to reconstruct an encryption key

by storing regeneration information at a trusted center. Consequently, Schwenk is focused on "encryption" keys. (See Col. 2, lines 28-67) and not authentication as claimed.

To clarify the focus of the present claims 29, 30, 43, and 44, these claims have been amended to recite "creating a private key, a public key corresponding to the private key, and an associated system parameter on the mobile user device", "wirelessly outputting the system parameter to a verifier device concurrent with wirelessly outputting the public key to the verifier device" and "using the private key for authentication of the mobile user device." Applicant submits that Schwenk fails to teach these limitations.

First, Schwenk is silent as to the operating environment in which its method is performed. That is, it fails to teach authentication between a *mobile user device* that *wirelessly communicates* with a verifier device. Consequently, Schwenk fails to disclose the recited limitations in these claims.

Secondly, Schwenk also fails to disclose that the *concurrent transmission of the system parameter and public key* as claimed. Because Schwenk fails to explicitly teach concurrent transmission of the public key and the system parameter as required under 102(e), it fails to teach this recited limitation.

Claim Rejections – 35 USC § 103

Claims 2, 15-18, and 23-25

The Office Action rejected claims 2, 15-18, and 23-25 under 35 U.S.C. §103(a) as being allegedly obvious in light of U.S. Patent No. 6,959,393 (hereinafter "Hollis") in view of Bruce Schneier's Applied Cryptography (hereinafter "Schneier").

The Office has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art references must teach or suggest all the claim limitations. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Third, there must be a reasonable expectation of success. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP § 2143 - § 2143.03 for decisions pertinent to each of these criteria.

Claimed Elements are Not Taught or Suggested by the Prior Art

Applicant submits that neither Hollis nor Schneier teach the claimed limitations where a mobile user device is authenticated by a network verifier device. In particular, the cited references fail to teach or suggest that a mobile user device generates and wirelessly transmits/outputs keys as claimed. For instance, Hollis appears to use an offline system to store the backup keys but it fails to disclose wireless distribution of such keys. Therefore, the claimed authentication system is a completely distinct system architecture than disclosed by the prior art.

No Motivation to Combine Cited References

Again, assuming, *arguendo*, that every claimed element is taught by the prior art, Applicants further submit that there is no motivation to combine Hollis and Schneier as alleged in the Office Action.

Specifically, Hollis uses an "offline backup" system to store the backup key (Col. 24, line 41) which is intended to restrict distribution of such backup key. By contrast, Schneier purposefully distributes different pieces of a key to different entities. These care completely opposite approaches to securing backup keys where Hollis secures the backup keys by keeping them "offline" while Schneier secures its backup key by transmitting it online in pieces to different entities. While both of these approaches protect the backup key, there is no explicit motivation to modify the teachings of Hollis to go from *offline* storage of the backup keys to the *online* distribution of the backup keys as in Schneier. The Final Office Action has not provided an objective motivation to combine these two opposing key security approaches and appears to *improperly rely on hindsight* and the disclosure of Applicant's claimed invention. Consequently, there is no motivation to combine the cited references.

No Reasonable Expectation of Success

Even if the references were combined, albeit improperly in Applicant's opinion, as described above, Applicant submits that there is no reasonable expectation of success in combining the cited prior art references Hollis and Schneier. Specifically, combining Hollis and Schneier does not involve a simple combination of features but would require a wholesale redesign or restructuring of the offline key security system taught by Hollis with an opposing online key security system taught by Schneier. Consequently, there is no reasonable expectation of success in combining these two references.

Consequently, prima facie obviousness has not been established as to these claims.

Claims 11-13, 19-21, 26-28, and 51

The Office Action rejected claims 11-13, 19-21, 26-28, and 51 under 35 U.S.C. §103(a) as being allegedly obvious in light of U.S. Patent No. 6,959,393 (hereinafter "Hollis") in view of US Publication 2002/0152380 (hereinafter "O'Shea").

Claimed Elements are Not Taught or Suggested by the Prior Art

Applicant submits that neither Hollis nor O'Shea teach the claimed limitations where a mobile user device is authenticated by a network verifier device. First, as noted above, Hollis fails to teach *wireless reception of keys* as claimed. Second, Hollis teaches that the backup keys are backed up (stored) *offline* not that they are *wirelessly received* as claimed. While Hollis does not disclose what such offline backup means, it is certainly opposite that online wireless transmission/reception of the backup keys claimed. Third, Hollis fails to teach the *concurrent reception of the first and second public keys* as claimed. Hollis discloses that the second public key backed up offline (Col. 24, line 41) and not transmitted with the first public key. O'Shea also fails to teach all of these claimed features. Consequently, Hollis and O'Shea, alone or in combination, fail to teach this limitation.

No Motivation to Combine Cited References

Again, assuming, *arguendo*, that every claimed element is taught by the prior art, Applicants further submit that there is no motivation to combine Hollis and O'Shea as alleged in the Office Action.

Specifically, Hollis uses an "offline backup" system to store the backup key (Col. 24, line 41) which is intended to restrict distribution of such backup key. By contrast, O'Shea purposefully distributes a public key from the mobile user device via a network (i.e., online distribution). These are opposite approaches to securing backup keys where Hollis secures the backup key by keeping it "offline" while O'Shea teaches online transmission of keys. There is no explicit motivation to modify the teachings of Hollis to go from *offline* storage of the backup keys to the *online* distribution of the backup keys as in O'Shea. The Final Office Action has not provided an objective motivation to combine these two opposing key security/distribution approaches and appears to *improperly rely on hindsight* and the disclosure of Applicant's claimed invention. Consequently, there is no motivation to combine the cited references.

No Reasonable Expectation of Success

Even if the references were combined, albeit improperly in Applicant's opinion, as described above, Applicant submits that there is no reasonable expectation of success in combining the cited prior art references Hollis and O'Shea. Specifically, combining Hollis and O'Shea does not involve a simple combination of features but would require a wholesale redesign or restructuring of the offline key security system taught by Hollis with an opposing online key security system taught by O'Shea. Consequently, there is no reasonable expectation of success in combining these two references.

Consequently, prima facie obviousness has not been established as to these claims.

Claims 3-10, 31-42, and 45-49

The remaining claims 3-10, 31-42, and 45-49 were rejected based on a combination of references, some of which are discussed above. Applicant has amended many of these claims to more clearly claim various features of the invention. Applicant submits that none of the cited prior art references teach the wireless distribution of a (backup) second public key from a mobile device concurrent with the wireless distribution of a first public key as claimed. The arguments and differences disclosed above apply equally to these claims and make the patentable over the cited prior art. In particular, none of the references disclose the *concurrent wireless transmission* of a first and second (backup) public key from a mobile user device to a verifier as claimed.

Based on at least the foregoing reasons, Applicant respectfully requests reconsideration and withdrawal of the rejection of, and/or objection and allowance of claims 1-51.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

Should any of the above rejections be maintained, Applicant respectfully requests that the noted limitations be identified in the cited references with sufficient specificity to allow Applicant to evaluate the merits of such rejections. In particular, rather than generally citing whole sections or columns, Applicant requests that the each claimed element be specifically identified in the prior art to permit evaluating the references.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Applicant requests a **three month** extension of time in which to respond to the Office Action dated October 24, 2007. Please charge extension any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Date: April 23, 2008

By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502